Docket No.: P2001,0019

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : BERNDT GAMMEL ET AL.

Filed : CONCURRENTLY HEREWITH

Title : CACHE MEMORY AND METHOD FOR ADDRESSING

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S i r :

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 101 01 552.6, filed January 15, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

LAURENCE A. GREENBERG
REG. NO. 29,308

For Applicants

Date: July 15, 2003

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/kf

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	101 01 552.6
Anmeldetag:	15. Januar 2001
Anmelder/Inhaber:	Infineon Technologies AG, München/DE
Bezeichnung:	Cache-Speicher und Verfahren zur Adressierung
IPC:	G 06 F 12/08

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. Juni 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Jerofsky

A 9161
06/00
EDV-L

Beschreibung

Cache-Speicher und Verfahren zur Adressierung

Die vorliegende Erfindung betrifft einen Cache-Speicher, der auf einem Security-Controller verwendet wird.

Cache-Speicher sind im allgemeinen relativ kleine, aber schnelle Pufferspeicher, die eingesetzt werden, um die Latenzzeit beim Zugriff eines Prozessors auf langsame externe Speicher zu reduzieren. Der Cache-Speicher überdeckt dabei ausgewählte Adressbereiche des externen Speichers und enthält die temporär modifizierten Daten sowie damit verbundene Informationen, wie z. B. Informationen zur Lokalisierung der Daten. Eine Übersicht über Cache-Speicher gibt der Artikel von Alan Jay Smith "Cache Memories" in Computing Surveys, Vol. 14, No. 3, September 1982, Seite 473 - 530. Die in Hardware realisierten Cache-Speicher können allgemein als ein N-way-set-assoziatives Speicherfeld charakterisiert werden. Dabei bedeuten die Grenzfälle N = 1 einen Speicher mit Direct Mapping und N = M einen voll-assoziativen Cache-Speicher, wobei M die Gesamtzahl der Einträge im Speicher bedeutet.

Im Allgemeinen werden die Daten in Blöcken von 2^b Bytes pro Speichereintrag gespeichert. Im allgemeinen Fall eines teilassoziativen Cache-Speichers mit $N = 2^n$ Wegen wird üblicherweise die p Bit breite Adresse des Datums so aufgeteilt, dass n Bit den Index, b Bit den Offset und die übrigen p - n - b Bit das Tag bilden. Das ist in der beigefügten Figur veranschaulicht.

Beim Zugriff auf ein Datum im Cache-Speicher, z. B. bei einem Lese- oder Schreibvorgang, wird das Index-Feld verwendet, um ein Set direkt zu adressieren. Das Tag-Feld wird zusammen mit dem jeweiligen Block abgespeichert, um ihn eindeutig innerhalb eines Sets zu identifizieren. Bei einer assoziativen Suche nach dem Block wird das Tag-Feld der Adresse mit den Tag-

Feldern in dem selektierten Set verglichen, um so den betreffenden Block aufzufinden. Der Offset-Eintrag wird benutzt, um das Datum im Block zu adressieren.

Derartige Cache-Speicher stellen auf Security-Controllern leicht zu identifizierende reguläre Strukturen dar. Damit bilden diese Cache-Speicher abgesehen von Busleitungen und Registersätzen bevorzugte physikalische Angriffspunkte für ein unbefugtes Ausspähen oder Manipulieren von sicherheitsrelevanten Daten, z. B. durch Nadelangriffe oder Ähnliches. In den externen Speichern werden üblicherweise sicherheitskritische Daten durch eine schwer zu decodierende Verschlüsselung geschützt, die z. B. in Hardware implementiert sein kann. Diese harte Ver- und Entschlüsselung mit entsprechenden Algorithmen führt auch bei einer Hardware-Implementierung zu einer hohen Latenzzeit im Betrieb des Speichers, die sich zur Latenzzeit des Speichers selbst addiert und dabei den überwiegenden Anteil darstellen kann. Eine derartige Verschlüsselung ist ungeeignet, da auf Cache-Speicher typischerweise in einem oder zumindest wenigen Taktzyklen zugegriffen werden können soll. Cache-Speicher stellen also einen Schwachpunkt im Sicherheitskonzept eines derartigen Security-Controllers dar, wenn sie nicht anderweitig geschützt werden.

Aufgabe der vorliegenden Erfindung ist es, eine Möglichkeit für eine wirkungsvolle und praktikable Sicherung eines Cache-Speichers auf einem Security-Controller anzugeben.

Diese Aufgabe wird mit dem Cache-Speicher mit den Merkmalen des Anspruches 1 bzw. mit dem Verfahren zur Adressierung eines Cache-Speichers mit den Merkmalen des Anspruches 3 gelöst. Ausgestaltungen ergeben sich aus den jeweiligen abhängigen Ansprüchen.

Bei dem erfindungsgemäßen Cache-Speicher sind Mittel vorhanden, die eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Tag-Teil der Adresse und einer verschlüsselten

Tag-Adresse vornehmen. Diese Mittel sind vorzugsweise als Hardware vorhanden. Das erfindungsgemäße Verfahren zur Adressierung wendet eine umkehrbar eindeutige Transformation zwischen einem Tag-Teil einer Cache-Adresse und einer verschlüsselten Tag-Adresse an, was vorzugsweise unter Einsatz von dafür vorgesehenen Mitteln geschieht, die als Hardware vorhanden sind.

Die erfindungsgemäße Lösung gibt durch Mittel und Verfahren eine Methode an, mit der das Sicherheitsniveau von Daten bzw. deren Adressen in Cache-Speichern erhöht werden kann, wobei die Zugriffszeit nicht oder allenfalls unwesentlich erhöht wird. Wie eingangs beschrieben wurde, werden in set-assoziativen Cache-Speichern Daten mittels eines Index-Feldes und eines Tag-Feldes abgelegt und abgerufen. Erfindungsgemäß wird eine umkehrbar eindeutige (ein-eindeutige) Abbildung benutzt, mit der das Tag-Feld der Adresse auf ein verschlüsseltes Tag-Feld abgebildet wird und umgekehrt. Blöcke werden dann im Cache-Speicher zusammen mit dem verschlüsselten Tag-Feld abgelegt. Auf diese Weise ist die Adressinformation für die Datenblöcke effizient geschützt. Die umkehrbar eindeutige Abbildung wird dabei durch eine dafür vorgesehene Hardware-Einheit durchgeführt. Diese wird bei bevorzugten Ausgestaltungen so ausgelegt, dass die Transformation innerhalb eines Taktzyklusses, d. h. on-the-fly, durchgeführt werden kann. Damit wird die Zugriffszeit auf den Cache-Speicher nicht erhöht.

Als weitere Ausgestaltung der Erfindung kann zusätzlich das Index-Feld der Adressen des Cache-Speichers durch eine weitere umkehrbar eindeutige Abbildung, die das Index-Feld auf ein verschlüsseltes Index-Feld abbildet, verschlüsselt werden. Auch dazu wird eine entsprechend vorzusehende Hardware-Einheit verwendet. Damit wird ein sogenanntes Set-Scrambling erreicht, bei dem der im Cache-Speicher zu verwaltende Block in einem nicht auf triviale Weise aufzufindenden Set abgelegt wird. Eine derartige Verschlüsselung wird vorzugsweise dann

zusätzlich durchgeführt, wenn die Architektur des Prozessors nicht vorsieht, dass auf Daten "unaligned" zugegriffen werden kann, so dass die Daten über die Blockgrenzen hinausragen.

Eine erfindungsgemäße Ausgestaltung eines Cache-Speichers ist insbesondere bei Cache-Speichern auf Sicherheitscontrollern (security-controller) bevorzugt.

Patentansprüche

1. Cache-Speicher,
dessen Adressen eine Aufteilung in Tag, Index und Offset aufweisen,
d a d u r c h g e k e n n z e i c h n e t , dass
Mittel vorhanden sind, die eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Tag-Teil der Adresse und einer verschlüsselten Tag-Adresse vornehmen.

2. Cache-Speicher nach Anspruch 1, bei dem
die Mittel zusätzlich eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Index-Teil der Adresse und einer verschlüsselten Index-Adresse vornehmen.

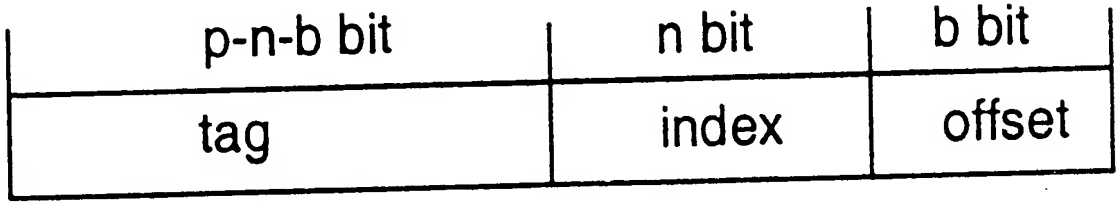
3. Verfahren zur Adressierung eines Cache-Speichers, bei dem eine umkehrbar eindeutige Transformation zwischen einem Tag-Teil einer Cache-Adresse und einer verschlüsselten Tag-Adresse vorgenommen wird.

4. Verfahren nach Anspruch 3, bei dem
zusätzlich eine umkehrbar eindeutige Transformation zwischen einem Index-Teil einer Cache-Adresse und einer verschlüsselten Index-Adresse vorgenommen wird.

Zusammenfassung

Cache-Speicher und Verfahren zur Adressierung

Bei dem Cache-Speicher, dessen Adressen in Tag, Index und Offset aufgeteilt sind, sind als Hardware Mittel vorhanden, die eine umkehrbar eindeutige Transformation zwischen dem jeweiligen Tag-Teil der Adresse und einer verschlüsselten Tag-Adresse vornehmen. Es kann zusätzlich das Index-Feld der Adressen des Cache-Speichers durch eine weitere umkehrbar eindeutige Abbildung, die das Index-Feld auf ein verschlüsseltes Index-Feld abbildet, verschlüsselt werden. Auch dazu wird eine entsprechend vorzusehende Hardware-Einheit verwendet.


p-n-b bit
n bit
b bit
tag
index
offset